Comment décrypter une clé WEP sous Windows

La protection de reseaux wifi par clé wep est dépassée et facilement contournable, même sous windows... C'est ce que nous allons vous montrer dans cet article en detaillant étape par étape comment hacker son propre réseau sans fil.

Préambule

Avertissement

Attention vous ne pouvez refaire ce qui est présenté sur cette page que si vous êtes le propriétaire du réseau ou à la rigueur si vous avez un accord certain de son propriétaire !!!

Le piratage est un fait grave et cet article n'est en aucun cas destiné à cette utilisation, il est simplement là pour vous sensibiliser à la sécurité de votre réseau.
Je le rappelle pour les pirates qui veulent à tout prix hacker leurs voisins:
vous encourez de fortes peines de prison et amendes si vous n'avez pas d'autorisation pour faire ce test!.

Matériel et programmes nécessaires

Il vous faut bien sûr un reseau sans fil cible .
Comme programmes je vais utiliser winaircrack de Hexanium (c'est une interface graphique pour aircrack qui sans çà serait beaucoup plus complexe à utiliser) et airodump pour la capture des paquets. Je vous conseille de prendre la version "pack" de winaircrack, sinon vous devrez télécharger aircrack et airodump séparement. Vous le trouverez facilement sur google.
Enfin il faut une carte wifi compatible avec airodump et c'est le plus dur. Il faut que la carte ait un chipset Atheros, Aironet, HermesI ou Realtek. Il y a differentes listes non exhaustives qui circulent sur le net mais la plupart du temps il faut faire aussi attention à la version de la carte (les cartes de [http://www.wildpackets.com/support/product_support/airopeek/hardware cette liste] sont compatibles).
Pour ma part, j'ai acheté une clé USB Wi-Fi sagem WL5061S sur ebay à 30€ car j'étais certain de sa compatibilitée avec airodump. C'est une des clé USB fournie avec la livebox de Wanadoo (mais ils ont aussi un autre modèle (sagem) qui ne marche pas, donc verifiez bien le modèle si vous voulez vous procurer celle-ci !).

Principe

Le decryptage d'une clé wep se divise en deux parties:

- la capture des paquets avec airodump : il faut récuperer un certain nombre de paquets cryptés qui circulent dans l'air. Pour celà, il faut qu'il y ait du traffic sur le reseau cible car sinon aucun paquet ne circulera ou très très peu et il faudra attendre des jours ou des semaines pour en avoir assez. Comme il s'agit de votre reseau ou que vous connaissez son proprio, vous pouvez transferer des gros fichier sur le reseau (copiez des fichiers d'un ordinateur à un autre ou téléchargez n'importe quoi).
- Le décryptage des paquets pour trouver la clé avec winaircrack. A partir du moment où vous avez récuperé assez de paquets à la première étape vous êtes sûr d'aboutir. Winaircrack va lui même lancer aircrack qui va chercher la clé wep.

Remarque importante sur les drivers

La plupart des drivers fournis par les constructeurs ne fonctionneront pas avec airodump pour la capture des paquets. Pensez donc à désinstaller votre carte wifi et à la réinstaller avec les drivers fournis sur le site wildpaquets (lien dans le paragraphe 1.2) ou bien avec les drivers génériques.

Vous gagnerez sans doute du temps en achetant une carte connue pour posséder des drivers permettant le mode "écoute", plutôt que d'essayer de trouver à tous prix des drivers pour votre carte réseaux. D'autant plus que le fait d'avoir deux cartes vous permet de vous connecter à un réseau de mauvaise réception mais ouvert, pendant que vous essayez de décrypter le réseau de bonne réception fermé (il est forcément de bonne réception étant donné que c'est le votre).

Capture des paquets

Configuration d'airodump

Après avoir réuni le matériel nécessaire et installé les bons drivers, simulez du traffic sur votre réseau pour gagner du temps et lancez airodump.

Voici le fonctionnement d'airodump étape par étape :

- **Known networks adaptaters** : affiche la liste de votre carte réseau (avec et sans fil), à vous de choisir la bonne, moi c'est celle qui a le numero 18 donc je tape '18'.
- **Interface Type** : choisissez celui qui correspond au chipset de votre carte en fonction des drivers que vous avez mis. Moi c'est les drivers générique donc j'ai mis 'a' et çà fonctionne
- **Channels** : Si vous savez sur quel canal votre wifi est émis saisissez le ici, sinon mettez 0, çà capturera sur tout les canaux. J'ai essayé les deux et j'ai eut un résultat nettement plus rapide en séléctionant mon canal.

Pages
Catégories
Uncategorized
Liste de Liens
Archive
décembre 2009
janvier 2008
Meta
Connexion
RSS
Commentaires RSS

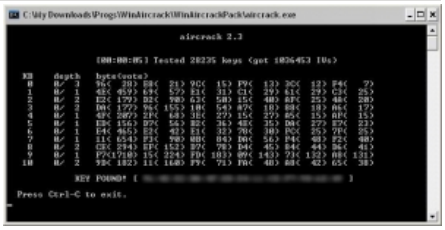
- **Output file name prefix** : Le nom de votre fichier qui contiendra les paquets capturés (exemple: 'monfichierdecapture').
- **Only write WEP IVs** : Ici vous choisissez si vous voulez capturer les paquets entiers ou juste les parties utiles au decryptage (ce qu'on appelle les IVs). Je vous conseille de mettre 'y' (pour 'yes') ainsi votre fichier final prendra simplement 6 Mo au lieu de plusieurs Gigas si vous mettez 'n'! A noter que si vous mettez 'y' le fichier aura l'extension .ivs et si vous mettez 'n' il aura l'extension .cap.

A propos d'airodump

Vous êtes maintenant normalement en train de capturer les paquets. Le nombre d'IVs capturés sont affichés dans la colonne "packets". Pour information et pour vous donner une éstimation du temps restant, il vous faut environ 300 000 IVs pour décrypter une clé 64bits et un peu plus d'un million d'IVs pour une clé 128bits... encore plus pour une 256bits. Cependant si vous êtes en train de transferer des gros fichiers sur le reseau avec un autre ordinateur vous devriez en avoir pour 2 heures environ. Pour arretter airodump, appuyez simultanement sur 'crtl'+'c'. Le fichier sera sauvegardé dans le repertoire d'airodump sous le nom que vous avez entré dans "Output file name prefix" précédement et portera l'extension '.ivs' .

- Si vous arrêtez la capture vous pourrez la continuer plus tard en specifiant le même nom de fichier qu'avant; ainsi il recommencera sans effacer ce qui a été capturé précédemment. Vous pouvez aussi créer un autre fichier et passer à l'étape suivant avec plusieurs fichiers.
- Vous pouvez passer à l'étape suivante (le décryptage) dès que vous avez 300 000 paquets au cas où la clé serait en 64bits tout en laissant tourner airodump. Ainsi si la clé n'est pas trouvé c'est qu'il vous faut plus de paquets mais vous n'avez pas perdu de temps puisque la capture n'a pas été arrentée.

Décryptage de la clé wep avec winaircrack



Lancez maintenant winaircrack :

- Dans l'onglet 'avancé' séléctionnez le chemin d'accès à aircrack.exe. Il se peut qu'il se soit mis bien automatiquement donc rien à modifier dans ce cas.
- Allez ensuite dans la partie 'générale' puis séléctionnez type d'encryption 'wep' (c'est celui-ci par default donc rien a modifier normalement) puis cliquez sur la petite icone pour ajouter un ou plusieurs fichiers de capture obtenus précédement avec airodump. Attention, lorsque la fenêtre s'ouvre pour rechercher le fichier, il faut changer en bas le 'type de fichier' car par default il recherche un fichier .cap; mettez donc .ivs ou 'tous les fichiers' sinon il n'apparaitra pas.
- Enfin cliquez sur 'aircracker' la clé... une fenêtre noire ms-dos va se lancer. Si il y avait plusieurs reseau actifs lors de la capture, il se peux qui vous ayez à choisir le votre (normalement c'est celui où il y a beaucoup plus de IVs que les autres). Vous n'avez plus qu'a attendre que la clé soit trouvée. Pour ma part, çà a pris 5 secondes mais il se peut que çà prennent quelques minutes.

Si cette étape échoue, vous n'avez certainement pas assez de paquets, continuez donc la capture avec airodump pour en récuperer plus. Parfois il faut presque 1,5 million de paquets pour une clé 128 bits et bcp plus pour une 256bits.

Conclusion

Vous l'avez certainement constaté si vous avez essayé de hacker votre réseau sans fil, les clés WEP offrent une sécurité bien mince. En effet, en envoyant beaucoup de fichiers sur le réseau, j'ai réussi à retrouver ma clé wep en 1h30. Il est clair que ce système de cryptage est largement dépassé et pourtant la majorité des réseaux wifi l'utilisent. Je vous conseille donc de passer au WPA(-PSK) qui offre une sécurité nettement meilleure que le WEP.

Complément

Verrouillage par adresse MAC

Je rajoute ce petit paragraphe pour ceux qui pensent que le filtrage des adresses mac est une securité suffisante. Détrompez-vous, il ne faut pas plus d'une minute pour en venir a bout.
Il faut tout d'abord capturer quelques paquets du reseau cible avec airodump mais cette fois ci, il ne faut pas choisir d'ecrire que les IVs donc quand on vous demande 'y' ou 'n' vous mettez 'n'. Un fichier .cap va être crée à la place du fichier .ivs qu'on avait avant. Ouvrez ce fichier avec ethereal; entrez la clé wifi decryptée un peu plus tôt dans les préférence d'ethereal (protocole->IIEE 802.11->clé wep). Vous pourrez ensuite lire les paquets et vous aurez l'adresse mac de l'ordinateur (ou des ordinateurs) qui est sur le reseau cible. Il ne reste plus qu'à mettre cette adresse comme adresse mac de votre carte reseau soit dans panneau de configuration/ gestionniares des peripheriques/votre carte wifi/ proriétés avancés... soit avec un petit programme pour changer les adresses mac. Redemarrez l'ordinateur et le tour est joué...

WPA & WPA2

Le WPA et le WPA2 n'ont à ce jour pas de faille connue. La seule méthode pour en venir à bout est d'utiliser des logiciels de bruteforce, c'est à dire d'utilisers des listes de mots de passe connus.

Il est donc très fortement déconseillé d'utiliser des mots de passes ayant une quelconque signification, les mot de passe comme "soleil", "vacance", "marjolaine", "bonbon", etc. sont totalement caduques. Choisissez plutôt des combinaisons de lettre, de chiffre et des ponctuations. Ainsi un mot de passe type "Calo4Er,PiO" est quasi impossible à décrypter.

Sous Linux

Sous Linux, la manipulation est quasiment identique. En effet, les logiciels sont exactement les même. Cependant, les drivers Linux offrent en plus des possibilité de réinjection de paquet. C'est à dire qu'ils permettent de vous faire passer pour quelqu'un d'autre et donc de pousser le routeur à regénérer des paquets intéressants.

C'est l'application aireplay qui est alors utilisée. Par cette méthode, vous pouvez réussir à attaquer n'importe quel clès 128 bits en moins de 15 minutes. Il vous suffit d'avoir 1 ou 2 adresses MAC de machines du réseau. Pour cette opération, je vous conseille de lancer une dizaine de processus d'AirReplay en simultanné. Le trafic généré sera alors colossal.

Une technique d'attaque que pourront effectuer certains méchants pirates sera d'utiliser tcpdump durant la journée pour récupérer le plus grands nombre d'adresses MAC de machines (à partir de fichiers de dump) puis d'envoyer 10 processus de aireplay durant la nuit à partir de ce dump du réseau. L'utilisateur ne voit alors pas son réseau perturbé (il dort), et l'attaquant est sur de récupérer la clès du réseau en moins de 15 minutes.

Les Live CD

Les Live CD sont des CD contenant un système (la plupart du temps à base de Linux) sur lesquels ont peut booter. Les Live CD de décryptage de réseau contiennent toutes les applications nécessaires au décryptage des réseaux WEP. Le gros avantage des Live CD, c'est que vous n'avez rien à installer et souvent la procédure est grandement simplifiée de façon à ce que vous y puissiez craquer le réseau en un temps aussi court que possible.

- BackTrack est un Live CD très récent. Beaucoup d'entre vous seront ravis d'apprendre que ce Live CD supporte les cartes Centrino. Il a entre autre la possibilité de faire démarrer d'autres machines sur le réseau pour faire des calculs partagés permettant de décrypter plus vite la clef WEP.
- L'ancienne distribution WHAX, dont BackTrack hérite en grande partie n'existe plus vraiment puisqu'elle n'a plus de site.

N'hésitez pas à laisser des commentaires pour nous permettre de corriger et/ou améliorer les articles du site.

Rating: 9.0/**10** (9 votes cast)

Rating: **+4** (from 8 votes)

Remplis sous: Uncategorized

Laisser un commentaire

Commentaires (6) Trackbacks (0) (Souscrire aux commentaires de cet article)

zonara
28 décembre 2009 - 14:42

Article toujours intéressant mais déjà bien rodé sur d'autres sites… Et puis les possibilités que nous laisse la distribution backtrack sont absolument incroyables. A ce sujet, on en est à la version 4 en bêta et non pas la version 2.

Rating: 3.7/**5** (3 votes cast)

Rating: **-5** (from 7 votes)

superfc
28 décembre 2009 - 19:17

C'est tout à fait vrai. En effet cet article n'est plus tout à fait à jour car il y a été écrit il y a plus de 5 ans, il était le premier à traiter de décryptage de clé WEP sous Windows.

J'essayerai de trouver un peu de temps pour le mettre à jour.

Rating: 5.0/**5** (1 vote cast)

Rating: **+2** (from 4 votes)

gerald
16 février 2010 - 21:06

bnsoir,
besoin d'aide svp….!
voila je voudrait tester la secu de mon livebox mais le souci c'est que quand j'use le aircrack il ne reconait pas ma carte wifi pourtant c'est du atheros meme ,quand au debut je tape la comande airmon-ng start wifi 0 il affiche quedal …..!dc si quelqu'un pourait m'aider ce serait cool!
thanks!!!!!

Rating: 0.0/**5** (0 votes cast)

Rating: **0** (from 0 votes)

superfc
17 février 2010 - 09:31

On pourrait potentiellement vous aider si vous donniez le modèle exacte de carte.

Rating: 0.0/**5** (0 votes cast)

Rating: **0** (from 0 votes)

flo
19 février 2010 - 22:03

Bonjour,moi g un probleme avec airodump quand je le lance aprés avoir rentré le canal du reseau et tapé y il m'affiche cela:the selected adaptator is not compatible with the PEEK protocol… j'utilise une carte reseau AR5006X et j'ai deja telecharger des fichiers peek.dll et peek5.sys avant de les avoir integrer dans win32 et dans aircrack … je ne comprend pas pourquoi cela ne marche pas avez vous une idée? merci d'avance

Rating: 0.0/**5** (0 votes cast)

Rating: **0** (from 0 votes)

arsene
21 février 2010 - 21:31

a pars win aircrak il nya pas un autre car g vraiment du mal a le télcharger

Rating: 0.0/**5** (0 votes cast)

Rating: **0** (from 0 votes)

Laisser un commentaire

Nom (requis)

Email (ne sera pas publié) (requis)

Site Web

Soumettre

« Installer Tomtom sur un Thomson Intuiva GPS280 Comment voler un Velib »

Copyright © 2010 LaPageDuJour · Propulsé par WordPress
Lightword Theme translated by Nouvelle Fraiches and Andrei Endurci

Aller en haut ↑